Vicki J. Maniatis, Esq.
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Phone: (212) 594-5300
vmaniatis@milberg.com

Terence R. Coates*
Justin C. Walker*
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

**Pro Hac Vice application forthcoming*

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

NICHOLAS KHIRFAN, individually and on behalf of all others similarly situated, Plaintiff, v. HEALTHEC, LLC, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Nicholas Khirfan ("Plaintiff)" brings this Class Action Complaint against HealthEC, LLC ("Defendant" or "HealthEC"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and at least 4,452,782[1] other similarly situated persons in a massive and preventable cyberattack where cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive Private Information belonging to Plaintiff and Class Members which was being kept unprotected (the "Data Breach").

2. Defendant failed to properly secure and safeguard Plaintiff's and Class Members' sensitive personally identifiable information ("PII")[2] including their full

[1] See *Cases Currently Under Investigation, U.S. Department of Health and Human Services, Office for Civil Rights* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Jan. 8, 2024).

[2] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its

names, Social Security numbers, addresses, dates of birth, and tax identification numbers, and protected health information ("PHI"), including medical information (including but not limited to diagnosis, diagnosis codes, mental/physical condition, prescription information, and provider's names and locations), health insurance information (including but not limited to beneficiary numbers, subscriber numbers, Medicaid/Medicare identification), billing and claims information (including but no limited to patient account numbers, patient identification numbers, and treatment cost information) (collectively, PII and PHI are "Private Information").

3. Plaintiff further seeks to hold Defendant responsible for not maintaining the Private Information in a manner consistent with industry standards.

4. Defendant is a population health management company the uses artificial intelligence to integrate clinical and claims data to create community health records for each patient.[3]

5. To provide these services for its customers, and in the ordinary course of Defendant' business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiff's and Class Members' Private Information.

face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[3] Homepage, HEALTHEC.COM, https://www.healthec.com/ (last visited Jan. 8, 2024).

6. While the Data Breach occurred between July 14, 2023 and July 23, 2023, Defendant did not begin informing victims of the Data Breach until December 22, 2023, 161 days later. On or about December 22, 2023, Defendant finally notified state Attorneys General and many Class Members about the widespread Data Breach via letter (the "Notice Letter").[4]

7. Plaintiff and Class Members were wholly unaware of the Data Breach until they received Notice Letters from Defendant. During this time, Plaintiff and Class Members were unaware that their sensitive Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

8. The Notice Letter provides no further information regarding the Data Breach and only recommends how victims can place a fraud alert or credit freeze on their account and how to sign up for the limited and abbreviated identity monitoring services Defendant offered in response to the Data Breach. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiff's and Class Members' Private Information remains in

[4] Sample Notice Letter available at the Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/4680936e-e496-43ed-a35d-59ece9b523b6/3a985a87-0cbb-4b2d-89f4-d0d1414d6e12/document.html (last visited Jan. 8, 2024).

the possession of criminals.

9. By acquiring, utilizing, and benefiting from Plaintiff's and Class Members' Private Information for its business purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiff and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiff's and Class Members' Private Information in its possession and to keep Plaintiff's and Class Members' Private Information confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

10. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiff's and Class Members' Private Information from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiff's and Class Members' Private Information.

11. Currently, the full extent of the types of Private Information, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

12. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement

adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiff's and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized criminal third party.

13. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

14. Based on the type of sophisticated and targeted criminal activity, the type of Private Information involved, and Defendant's admission that the Private Information was accessed and copied, it can be concluded that the unauthorized criminal third party was able to successfully target Plaintiff's and Class Members' Private Information, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiff's and Class Members' Private Information for the purposes of utilizing or selling the Private Information for use in future fraud and identity theft related cases.

15. As a result of Defendant's failures and the Data Breach, Plaintiff' and Class Members' identities are now at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

16. As Defendant instructed, advised, and warned in its Notice Letter discussed below, Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

17. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant' warnings and following its instructions in the Notice Letter; (g) deprivation of value of their Private Information; (h) invasions of their privacy; and (i) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect it.

18. Plaintiff brings this action on behalf of all persons whose Private Information was compromised due to Defendant's failure to adequately protect Plaintiff's and Class Members' Private Information.

PARTIES

19. Plaintiff Nicholas Khirfan is an adult individual and, at all relevant times herein, a resident and citizen of the state of Michigan, residing in Royal Oak, Michigan.

20. Defendant HealthEC, LLC is a limited liability company formed under the state laws of Delaware, with its principal place of business at 343 Thornall Street, Suite 630, Edison, Middlesex County, New Jersey 08837.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff Khirfan, is a citizen of a state different from Defendant.

22. This Court has general personal jurisdiction over Defendant HealthEC because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

23. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District; Defendant maintains Class Members' Private Information in this District; and Defendant caused harm to Class Members residing in this District, including accessing and copying Private Information of patients of University Medical Center of Princeton Physician's Organization which is located in Somerset County, New Jersey.

HEALTHEC'S BUSINESS

24. Defendant HealthEC is a population health technology company that provides services to other companies. Defendant provides "fully integrated analytics and insights" and other services to its healthcare provider clients.[5]

25. HealthEC contracts with healthcare systems and providers "to identify high-risk patients, close care gaps and recognize barriers to optimal care."[6]

26. As a condition of providing services to its customers, Defendant requires that it customers entrust it with the Private Information belonging to its customer's patients. Defendant then acquires, possesses, analyzes, and otherwise utilizes Plaintiff's and putative Class Members' Private Information.

27. Defendant has served thousands of individuals since its founding and has created and maintains a massive repository of Personal Information, acting as a particularly lucrative target for data thieves looking to obtain, misuse, or sell patient data.

28. In the ordinary course of its business, HealthEC maintains the Private Information of its customers' current and past patients including but not limited to full names, Social Security numbers, addresses, dates of birth, tax identification

[5] *Homepage,* https://www.healthec.com/ (last visited Jan. 8, 2024).

[6] *Id.*

numbers, medical information (including but not limited to diagnosis, diagnosis codes, mental/physical condition, prescription information, and provider's name and location), health insurance information (including but not limited to beneficiary numbers, subscriber numbers, Medicaid/Medicare identification), and billing and claims information (including but no limited to patient account numbers, patient identification numbers, and treatment cost information).

29. As a HIPAA covered business entity (*see infra*), HealthEC is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Personal Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

30. However, HealthEC did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited 161 days to disclose the Data Breach publicly.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

32. At every step, Defendant stores Plaintiff's and Class Members' Private

Information and has a duty to protect that Private Information from unauthorized access.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

34. Defendant's Privacy Policy, posted on its website, describes how confidential patient information is used and disclosed. Defendant's Privacy Policy states that HealthEC "has implemented generally accepted standards of technology and operational security in order to protect Personal Info from loss, misuse, alteration, or destruction. Only authorized HealthEC personnel are provided access to Personal Info, and these employees are required to treat this information as confidential."[7]

35. Due to Defendant's substantial experience in handling highly sensitive Private Information, Defendant understood the need implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use the Private Information solely for proper business and healthcare related services and purposes, and to prevent the unauthorized

[7] *Privacy Policy*, https://mneconnect.healthec.com/ProdMNeConnectAdmin/Privacy_Policy.aspx (last visited Jan 8, 2024).

disclosure of the Private Information.

HealthEC is a HIPAA Covered Entity

36. HealthEC is a healthcare provider covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (see 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

37. As a regular and necessary part of its business, HealthEC collects and custodies the highly sensitive Private Information of its clients' patients. HealthEC is required under federal and state law to maintain the strictest confidentiality of the patient's Private Information that it requires, receives, and collects, and HealthEC is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

38. As a HIPAA covered entity, HealthEC is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including

incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

39. Due to the nature of HealthEC' business, HealthEC would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

40. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, HealthEC assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

41. Plaintiff and Class Members are patients, or former patients, of HealthEC's customers. HealthEC collected, aggregated, and maintained Plaintiff's and Class Members' Private Information on their computer networks.

42. Plaintiff and the Class Members relied on HealthEC to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information. HealthEC Plaintiff and Class Members reasonably expected that HealthEC would safeguard and keep their Private Information confidential.

43. As described throughout this Complaint, HealthEC did not reasonably protect, secure, or store Plaintiff's and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information HealthEC maintained. Consequently, cybercriminals circumvented HealthEC's security measures, resulting in a significant data breach.

The Data Breach and Notice Letter

44. HealthEC detected unauthorized access to certain computer systems within its network environment. The unauthorized access was the result of a cybersecurity incident.[8]

45. HealthEC took steps to secure its network systems and investigated the nature and scope of the incident with the consultation of third-party cybersecurity professionals.[9]

46. Through its investigation, HealthEC determined that its network and servers were subject to a cyberattack between July 14, 2023 and July 23, 2023, that impacted its network resulting in information on its network being accessed and

[8] *See* Notice Letter

[9] *Id.*

copied without authorization.[10]

47. Upon information and belief, Plaintiff's and Class Members' Private Information was copied, exfiltrated, and stolen in the attack.

48. Furthermore, the investigation determined that the accessed systems contained Private Information. Upon information and belief, this Private Information was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

49. The type of Private Information accessed by the unauthorized actor in the Data Breach includes full name, Social Security number, address, date of birth, tax identification number, medical information (including but not limited to diagnosis, diagnosis code, mental/physical condition, prescription information, and provider's name and location), health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification), and billing and claims information (including but no limited to patient account number, patient identification number, and treatment cost information).[11]

50. While HealthEC stated in the Notice Letter that the unusual activity

[10] *Id.*

[11] *Id.*

occurred between July 14, 2023 and July 23, 2023, HealthEC did not begin notifying victims until December 22, 2023, 161 days after HealthEC discovered the Data Breach occurred.[12]

51. Defendant had obligations created by contract, industry standards, HIPPA, common law, and its own promises and representations to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

52. Plaintiff and Class Members provided their Private Information directly, or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

53. Through its Notice Letter, HealthEC also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing financial accounts, and reviewing credit reports for possible fraud.

54. HealthEC has offered abbreviated, non-automatic credit monitoring services to victims thereby identifying the harm posed to Plaintiff and Class Members as a result of the Data Breach, which does not adequately address the

[12] *Id.*

lifelong harm that victims face following the Data Breach. Indeed, the Data Breach involves Private Information that cannot be changed, such as Social Security numbers.

55. Beginning on or around December 22, 2023, Defendant issued Notice Letters to Plaintiff and Class Members. In total, Defendant reported that the Private Information belonging to at least 4,452,782 individuals was compromised in the Data Breach.[13]

56. The Notice Letters sent to Plaintiff and Class Members stated Private Information, including full names, Social Security numbers, addresses, dates of birth, tax identification numbers, medical information (including but not limited to diagnosis, diagnosis code, mental/physical condition, prescription information, and provider's name and location), health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification), and billing and claims information (including but no limited to patient account number, patient identification number, and treatment cost information) were accessed and exfiltrated in the Data Breach.

[13] See *Cases Currently Under Investigation, U.S. Department of Health and Human Services, Office for Civil Rights* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Jan. 8, 2024).

57. As a result of the Data Breach, Plaintiff and 4,452,782 Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

58. Defendant waited 161 days to disclose the Data Brach to Plaintiff and Class Members. As a result of this delay, Plaintiff and Class Members had no idea their Private Information had been compromised in the Data Breach, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

59. Defendant's failure to timely detect and report the Data Breach made Plaintiff and Class Members vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

60. Plaintiff's and Class Members' Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information.

61. As a HIPAA covered entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk

of which HealthEC was aware and knew it had a duty to guard against. It is well-known that healthcare businesses such as Defendant, which collect and store the confidential and sensitive PII/PHI of thousands of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

62. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

63. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect the Private Information it maintains or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' Private Information.

64. Plaintiff and Class Members indirectly entrusted Defendant with sensitive and confidential information, including their Private Information which includes information that is static, does not change, and can be used to commit myriad financial crimes.

65. Plaintiff and Class Members relied on Defendant to keep their Private

Information confidential and securely maintained, to use their Private Information for authorized purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their Private Information.

66. The unencrypted Private Information of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

67. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information.

68. Due to Defendant's inadequate security measures and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

The Data Breach Was Foreseeable

69. Defendant's data security obligations were particularly important given

the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

70. At all relevant times, HealthEC knew, or should have known, that Plaintiff and Class Members' Private Information was a target for malicious actors. Despite such knowledge, HealthEC failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that HealthEC should have anticipated and guarded against.

71. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

72. In light of recent high profile data breaches at other health care providers, Defendant knew or should have known that their electronic records and the Private Information Defendant maintained would be targeted by cybercriminals and ransomware attack groups.

73. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the

758 medical data breaches that Protenus compiled in 2020.[14]

74. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[15]

75. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

76. Indeed, cyberattacks against the healthcare industry have been common

[14] *2022 Breach Barometer*, PROTENUS, *see* https://blog.protenus.com/key-takeaways-from- the-2022-breach-barometer (last visited Jan. 8, 2024).

[15] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available at: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited Jan. 8, 2024).

for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[16]

77. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[17] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[18] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[19]

78. Cyberattacks on medical systems like Defendant have become so

---

[16] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited Jan. 8, 2024).

[17] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?,* HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited Jan. 8, 2024).

[18] *Id.*

[19] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited Jan. 8, 2024).

notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[20]

79. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents." [21]

80. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical

[20] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Jan. 8, 2024).

[21] https://www.hipaajournal.com/why-do-criminals-target-medical-records/(last visited Jan. 8, 2024).

and clinical data, and that information can be easily monetized."[22]

81. Patient records, like those stolen from HealthEC, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[23]

82. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

83. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[24]

84. HealthEC was on notice that the FBI has expressed recent concern about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare

[22] See *id.*

[23] See *id*.

[24] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack*

industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[25]

85. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it is a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[26]

86. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

87. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive personal

---

[25] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited Jan. 8, 2024).

[26] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Jan. 8, 2024).

information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[27]

88. As a HIPAA covered entity, HealthEC should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

Defendant Fails to Comply with FTC Guidelines

89. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

90. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer

[27] https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops (last visited Apr. 7. 2023).

needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[28] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[29]

91. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

92. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from

[28] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2022).

[29] *Id.*

these actions further clarify the measures businesses must take to meet their data security obligations.

93. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

94. Defendant failed to properly implement basic data security practices.

95. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

96. Defendant was at all times fully aware of its obligation to protect the Private Information of customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

97. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

98. Several best practices have been identified that at a minimum should be

implemented by healthcare providers like Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

99. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

100. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

101. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these

accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Defendant's Conduct Violates HIPAA Obligations to Safeguard Private Information

102. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

103. HealthEC is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

104. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

105. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

106. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under

authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

107. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

108. The Data Breach resulted from a combination of insufficiencies that demonstrate HealthEC failed to comply with safeguards mandated by HIPAA regulations.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

109. Cyberattacks and data breaches at healthcare companies and partner companies are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

110. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the

months and years after the attack.[30]

111. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[31]

112. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[32]

113. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a

[30] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited Jan. 8, 2024).

[31] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[32] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 8, 2024).

puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

114. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[33]

115. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

[33] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 8, 2024).

116. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

117. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[34]

118. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

119. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

[34] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

120. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
> *See* GAO Report, at p. 29.

121. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

122. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

123. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

124. Private Information can sell for as much as $363 per record according to the Infosec Institute.[35] Private Information is particularly valuable because

[35] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 8, 2024).

criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

125. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[36] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[37] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

126. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

127. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social

[36] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 8, 2024).

[37] *Id.*

Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[38]

128. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[39]

129. Medical information is especially valuable to identity thieves.

130. Theft of PHI is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the data thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[40]

---

[38] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Jan. 8, 2024).

[39] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 8, 2024).

[40] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 8, 2024).

131. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

132. According to Flashpoint Services, Social Security numbers were selling on the dark web for $4 in 2020.[41] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[42]

133. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

134. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

135. Defendant breached its obligations to Plaintiff and Class Members

---

[41] *See* Jesse Damiani, Your Social Security Number Costs $4 on the Dark, Forbes.com (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=39b34a3013f1 (last visited Jan. 8, 2024).

[42] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Jan. 8, 2024).

and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access

rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain

security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

136. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Defendant' computer network and systems which contained unsecured and unencrypted Private Information.

137. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Defendant's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

138. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

139. Defendant admitted that the Data Breach occurred between July 14, 2023 and July 23, 2023. However, Defendant did not start notifying affected individuals until at least December 22, 2023, nearly 161 days later. Even then, Defendant provided only vague information as to exactly what types of Private Information was accessed and Defendant did not disclose the timeframe which cybercriminals were present on Defendant's network. As a result, Plaintiff and Class Members are unsure as to the scope of information that was compromised and the risks they face.

140. Defendant's failure to timely notify the victims of its Data Breach meant that Plaintiff and Class Members were unable to take affirmative measures to prevent or mitigate the resulting harm.

Plaintiff's and Class Members' Damages

141. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for the rest of their lives. Yet, to date, Defendant has merely offered to provide victims of the Data Breach with limited, abbreviated

subscriptions to identity monitoring services. This does nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Nor will it prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach. And at the conclusion of these limited subscriptions, victims will be required to pay for such services out of their own pocket.

142. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

143. Plaintiff's and Class Members' full names, Social Security numbers, addresses, dates of birth, tax identification numbers, medical information (such as diagnosis, diagnosis codes, mental/physical condition, prescription information, and provider's name and location), health insurance information (such as beneficiary numbers, subscriber numbers, Medicaid/Medicare identification), billing and claims information (including but no limited to patient account numbers, patient identification numbers, and treatment cost information) were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

144. Since being notified of the Data Breach, Plaintiff Khirfan has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

145. Due to the Data Breach, Plaintiff anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

146. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

147. As a direct and proximate result of Defendant' conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

148. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

149. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

150. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

151. Plaintiff and Class Members may also incur out-of-pocket costs for

protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

152. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

153. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant's customers was intended to be used by Defendant to fund adequate security of HealthEC's computer system(s) and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

154. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their medical accounts and sensitive information for misuse.

155. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred

to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for the rest of their lives.

156. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

157. Further, as a result of Defendant's conduct, Plaintiff and Class

Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

158. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiff's Individual Experience

Plaintiff Nicholas Khirfan's Experience

159. At the time of the Data Breach, Defendant retained Plaintiff Khirfan's Private Information in its system.

160. Plaintiff Khirfan was sent a Notice Letter dated December 22, 2023, informing him that Defendant had experienced a Data Breach and that Plaintiff's Private Information, including his full name, Social Security number, address, date of birth, medical information (such as diagnosis, diagnosis code, mental/physical condition, prescription information, and provider's name and location),health insurance information (such as beneficiary number, subscriber number, Medicaid/Medicare identification),and/or billing and claims information (including but not limited to patient account number, patient identification number, and

treatment cost information) was compromised in the Data Breach.

161. Plaintiff Khirfan's Private Information has already been stolen and misused as he has experienced incidents of fraud and identify theft. Shortly after, and as a result of the Data Breach, Plaintiff Khirfan discovered that his identity had been stolen when an unauthorized third party opened a fraudulent bank account in Plaintiff's name at Varo Bank.

162. After discovering the fraudulent bank account, Plaintiff then spent numerous hours on the phone and through email with Varo Bank, an internet only bank, to close the fraudulent bank account opened in his name.

163. As a result of the Data Breach, Plaintiff Khirfan spent time dealing with the consequences of the Data Breach, which includes placing a security freeze on his credit reports, verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and/or credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff Khirfan to mitigate his damages by, among other things, freezing his credit accounts and monitoring his accounts for fraudulent activity.

164. Plaintiff Khirfan regularly takes steps to safeguard him own Private Information in his own control.

165. Plaintiff Khirfan is a cautious person and is therefore very careful about

sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Khirfan stores any documents containing his Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Khirfan diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

166. The Data Breach caused Plaintiff Khirfan to suffer a loss of privacy.

167. Plaintiff Khirfan has also experienced an increase in the number of spam calls and emails since the Data Breach.

168. The Data Breach has caused Plaintiff Khirfan to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

169. As a result of the actual harm Plaintiff Khirfan has already suffered, and the substantial present risk of additional harm that he will face the rest of his life, Plaintiff Khirfan spent valuable keeping his credit reports frozen with all three major credit bureaus.

170. The loss of privacy and substantial present risk of additional imminent harm have caused Plaintiff Khirfan to suffer stress, fear, and anxiety as Plaintiff

Khirfan is very concerned that his sensitive Private Information is now in the hands of data thieves and shall remain that way for the remainder of his lifetime and there is nothing Plaintiff Khirfan can do to retrieve his stolen Private Information from the cyber-criminals.

171. Given the time Plaintiff Khirfan has lost investigating this data breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Khirfan's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Khirfan's valuable Private Information, the damages articulated more specifically above are far from the full extent of the harm thereto.

CLASS ALLEGATIONS

172. Plaintiff brings this nationwide class action individually and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

173. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All United States residents whose Private Information was compromised during the Data Breach (the "Class").**

174. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors,

and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

175. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

176. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are at least multiple thousands of individuals who were notified by Defendant of the Data Breach. According to the report submitted to the Department of Health and Human Services Office for Civil Rights, 4,452,782 individuals had their Private Information compromised in this Data Breach.[43] The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

177. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and

[43] See *Cases Currently Under Investigation, U.S. Department of Health and Human Services, Office for Civil Rights* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Jan. 8, 2024).

fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

178. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

179. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on

grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

180. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

181. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence,

effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

182. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

183. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable

identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

184. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

185. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

186. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

187. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's

wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

188. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 187.

189. Defendant required Plaintiff and class members Private Information as a condition of receiving healthcare services and to perform Defendant's AI-driven analytics in connection with providing medical treatment. Defendant collected and stored the data for purposes of providing medical treatment as well as for commercial gain. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

190. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

191. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the

Class, even if the harm occurred through the criminal acts of a third party.

192. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

193. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain.

194. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

195. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant, either directly or indirectly, with their confidential Private Information, a necessary part of obtaining services from Defendant.

196. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

197. A breach of security, unauthorized access, and resulting injury to

Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

198. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

199. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

200. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

201. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

202. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession

might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

203. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

204. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

205. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

206. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

207. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

208. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

209. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information it was no longer required to retain pursuant to regulations.

210. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

211. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

212. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

213. Defendant's duty of care to use reasonable security measures arose as

a result of the special relationship that existed between Defendant and consumers and patients, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

214. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

215. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

216. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was

particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

217. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

218. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

219. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

220. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of

the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

221. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

222. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

223. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF THIRD-PARTY BENFICIARY CONTRACT
(On behalf of Plaintiff and the Class)

224. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 187 above as if fully set forth herein.

225. Acting in the ordinary course of business, HealthEC entered into contracts with health systems to provide AI-enabled, population health management services using patients' PHI received from the health system.

226. Upon information and belief, each of those respective contracts contained provisions requiring Defendant to protect the patient information that Defendant received in order to provide such population health management services in carrying out the business.

227. Upon information and belief, these provisions requiring Defendant acting in the ordinary course of business to protect the personal information of the third-party patient's was intentionally included for the direct benefit of Plaintiff and class members, such that Plaintiff and class members are intended third party beneficiaries of these contracts, and therefore entitled to enforce them.

228. Defendant breached these contracts while acting in the ordinary course of business by not protecting Plaintiff's and class member's personal information,

as stated herein.

229. As a direct and proximate result of Defendant's breaches, Plaintiff and class members sustained actual losses and damages described in detail herein. Plaintiff and class members alternatively seek an award of nominal damages.

COUNT III
Unjust Enrichment
(On behalf of Plaintiff and the Class)

230. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 187. Notwithstanding, Plaintiff brings this claim in the alternative to any claim for breach of contractual obligations.

231. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of payments for medical and healthcare services, including those paid indirectly by Plaintiff and Class Members to Defendant.

232. Defendant benefited from receiving Plaintiff's and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

233. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

234. Defendant was also enriched from the value of Plaintiff's and Class Members' Private Information. Private Information has independent value as a form

of intangible property. Defendant also derives value from this information because it allows Defendant to operate its business and generate revenue.

235. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

236. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

237. Defendant acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

238. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

239. Plaintiff and Class Members have no adequate remedy at law.

240. As a direct and proximate result of Defendant's conduct, Plaintiff and

Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

241. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

242. Defendant should be compelled to disgorge into a common fund or

constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

243. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 187.

244. Defendant invaded Plaintiff's and the Class Members' right to privacy by allowing the unauthorized access to Plaintiff's and Class Members' Private Information and by negligently maintaining the confidentiality of Plaintiff's and Class Members' Private Information, as set forth above. Defendant further invaded Plaintiff's and Class Member's privacy by giving publicity to Plaintiff's and Class Members sensitive and confidential Private Information.

245. The intrusion was offensive and objectionable to Plaintiff, the Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiff's and Class Members' Private Information was disclosed without prior written authorization of Plaintiff and the Class.

246. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class Members provided and disclosed their Private Information to Defendant privately with an intention that the Private Information would be kept confidential and protected from unauthorized disclosure.

Plaintiff and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

247. As a direct and proximate result of Defendant's above acts, Plaintiff's and the Class Members' Private Information was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class Members suffered damages as described herein.

248. Defendant has committed oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class Members' Private Information with a willful and conscious disregard of Plaintiff's and the Class Members' right to privacy.

249. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and Class Members' Private Information with sub-standard and insufficient protections.

250. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class Members great and irreparable injury in that the Private Information maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or

local laws;

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security

monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its

respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to

counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: January 9, 2024

Respectfully Submitted,

/s/ Vicki J. Maniatis

Vicki J. Maniatis, Esq.
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Phone: (212) 594-5300
vmaniatis@milberg.com

Terence R. Coates (*pro hac vice forthcoming*)
Justin C. Walker (*pro hac vice forthcoming*)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530

Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com

Counsel for Plaintiff and Putative Class